

REMARKS

In the Office Action, the Examiner issued a final rejection of Claims 1-14 under 35 U.S.C. §103 as being unpatentable over the prior art, principally U.S. Patents 5,592,553 (Guski, et al.) and 6,141,760 (Abadi, et al.). Claims 15 and 16 were allowed.

More specifically, Claims 1, 6 and 8-10 were rejected as being unpatentable over Guski, et al. in view of Abadi, et al; and Claims 2, 7, 11 and 14 were rejected as being unpatentable over Guski, et al. and Abadi, et al. and further in view of portions of a textbook "Applied Cryptography" (Schneier). Claims 3-5, 12 and 13 were rejected over Guski, et al. in view of Abadi, et al. and further in view of a reference identified as "Cheng."

Cheng has not been further identified either in this Office Action or in the previous Office Action. Applicant requests that the Examiner identify this reference more specifically.

Applicant herein also asks that independent Claims 1 and 10 be amended to better define the subject matters of these claims. Claim 14 is being amended to correct a minor informality.

For the reasons discussed below, Claims 1-14 patentably distinguish over the prior art and are allowable. The Examiner is thus requested to enter this Amendment, to reconsider and to withdraw the rejections of Claims 1-14, and to allow these claims.

The present invention, generally, relates to a method and device for reading in a password to a computer system and encrypting that password. The use of computer passwords has become very common. Despite this, there are a number of problems with the use of computer passwords.

For instance, one important problem that is effectively addressed by this invention is the use of rouge software, such as a Trojan Horse, to hijack or steal a password when it is entered into the computer. The present invention effectively addresses this problem by putting a software generator module in the operating system of the computer, in series between a user who is inputting the password and the program being accessed. This generator module encrypts the password, and then the encrypted password is sent to the program, allowing access to that program.

Guski, et al. and Abadi, et al, describe procedures and system for improving the security of passwords.

For example, Guski, et al. describes a procedure in which passwords are used one-time only. The passwords change pseudorandomly, for example as a function of time, with each request for authentication. In this procedure, at a requesting node, a non-time dependent value is generated from nonsecret information identifying the user and a host application, using a secret encryption key shared with an authenticating node. This non-time dependent value is combined with a time-dependent value to generate a composite value that is encrypted to produce an authentication parameter. This authenticating password is reversibly transformed into an alphanumeric character string that is transmitted as a one-time password to the authenticating node. The advantage of using such a one-time password is that, even if the password is intercepted, it cannot be later used to gain access to the computer system.

Abadi, et al. describes a method for generating unique passwords. In the disclosed process, several values, for example, a master password, an access password and a user name, are combined to produce a unique password. In this way, common

passwords or passwords that might be used by more than one person, are converted to unique passwords.

There are a number of important differences between these prior art references and the present invention. One significant difference is that, with the present invention, the program requesting the password sends to the computer system an encrypted program-specific identifier. The computer system then use that encrypted identifier to encrypt the entered password to generate an encrypted program and password specific identifier. This latter identifier is then sent back to the requesting program, which can process the encrypted program and password specific identifier to authenticate the password.

Independent Claims 1 and 10 describe the above-discussed feature of the invention. In particular, both of these claims describe a computer including an operating system having a generator module, and both of these claims indicate that the generator module receives an encrypted program specific identifier from a program, receives the password, and uses the encrypted program specific identifier to encrypt the password to generate an encrypted program-password-specific identifier.

As discussed above, neither Guski, et al. nor Abadi, et al discloses or suggests this feature of the invention.

The other references of record have been reviewed, and they to, whether considered individually or in combination, also do not disclose or suggest this use of a generator module.

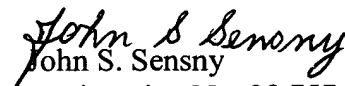
In particular, it is noted that Schneier discloses encryption processes. It is important to recognize, though, that the present invention is not simply the use of an encryption process, but is the use of an encryption process to encrypt specific information in a particular way to achieve a specific result – and in particular, to use the encrypted program specific identifier to encrypt the user password to generate an encrypted program-password-specific identifier, which can then be used by the requesting program to authenticate the password.

Because of the above-discussed differences between Claims 1 and 10 and the prior art, and because of the advantages associated with these differences, Claims 1 and 10 patentably distinguish over the prior art and are allowable. Claims 2-7 and 14 are dependent from Claim 1 and are allowable therewith; and Claims 11-13 are dependent from, and are allowable with, Claim 10. Also, Claims 8 and 9 incorporate by reference the method steps described in Claim 1, and thus Claims 8 and 9 patentably distinguish over the prior art for the same reasons advanced above in connection with Claim 1.

The amendments requested herein only emphasize or re-phrase features already described in Claims 1 and 10. For example, both of these claims already describe the program-specific identifier, the password, and generating a program-password specific identifier, and the present amendment only elaborates on these features or elements of the claims. Accordingly, it is believed that entry of this Amendment is appropriate, and such entry is respectfully requested.

In light of the foregoing, the Examiner is respectfully asked to enter this Amendment, to reconsider and to withdraw the rejections of Claims 1-14 under 35 U.S.C. §103, and to allow these claims. If the Examiner believes that a telephone conference with Applicant's Attorneys would be advantageous to the disposition of this case, the Examiner is asked to telephone the undersigned.

Respectfully submitted,


John S. Sensny
Registration No. 28,757
Attorney for Applicant

SCULLY, SCOTT, MURPHY & PRESSER
400 Garden City Plaza – Suite 300
Garden City, New York 11530
(516) 742-4343

JSS:jy